AFFIDAVIT OF FBI SPECIAL AGENT CRAIG A. GRAHAM

Introduction

I, Craig A. Graham, having been duly sworn, state as follows:

1. Since 2010, I have been a special agent with the Federal Bureau of Investigation ("FBI"). Early in my career, I focused on counterintelligence investigation. Starting in 2015, my responsibilities expanded to include the investigation of wire fraud, mail fraud, and other white collar offenses, and since July 2018, when I was assigned to the FBI's Providence Resident Agency, I have focused primarily on white collar investigation. I have experience in the investigation of telemarketing fraud, and through that work have gained a familiarity with computer or smartphone based communication applications such as WhatsApp, Snapchat, and Skype.

2. I submit this affidavit in support of a criminal complaint and arrest warrant charging Sahil Narang (born August 1991), who resides in India, with the following offenses:

(i) wire fraud, in violation of 18 U.S.C. §§ 1343,

(ii) bank fraud, in violation of 18 U.S.C. §§ 1344,

(iii) telemarketing or email marketing fraud, in violation of 18 U.S.C. §§ 2326, and

(iv) conspiracy to commit and/or attempt the aforementioned frauds, in violation of 18 U.S.C. § 1349.

3. The information in this affidavit comes from my personal observations and investigation, my training and experience, other law enforcement agents, an FBI source of information, and other sources as specified in the body of this affidavit. This affidavit is intended to show that there is sufficient cause for the requested warrant and does not set forth all of my knowledge about this matter or investigation.

Investigation

August 2018

4. In August 2018, a covert source of information (the "Informant") told me that an acquaintance, an Indian male named Sahil Narang ("Narang"), was defrauding people who resided in the United States. The Informant said that Narang had call center workers in India telephone United States residents and directed them, under false pretenses, to transfer money to the participants in the scheme. The Informant said that prior to becoming a source of information for the FBI, he had met Narang through a mutual acquaintance and visited Narang in India.

5. The Informant provided me the Facebook identification number for Narang's Facebook account. I know from my training and experience that each Facebook user account is commonly assigned a unique identification number that can be used to navigate to the associated user's profile page. Entering the provided identification number in my browser led me to a Facebook profile page for a "Sahil Narang." The Informant identified that profile as belonging to Narang and identified Narang as the person in the profile picture. According to Narang's profile page, he lives in "Gurgaon, Haryana." Gurgaon is an Indian city approximately 20 miles southwest of New Delhi and is located in the north Indian providence of Haryana.[1] Attached as Exhibit 1 is a screen shot of Narang's profile page, and the second page of the exhibit is an enlarged version of the profile picture.

6. I searched an FBI database that included visa records, specifically information and materials provided by or on behalf of those seeking visas to enter the United States. There was an entry for a visa applicant named "Sahil Narang" (and was born in August, 1991), and there is sufficient cause to believe that that applicant was Narang:

- The application included a photograph of the applicant, and the Informant identified Narang as the person photographed.
- The person in the photograph is consistent in appearance with the Facebook profile picture, which is attached as Exhibit 1.

[1] The last publicly viewable post on Narang's Facebook profile page is dated July 19, 2017.

- The application listed place of birth as "Gurgaon" and place of residence as "Gurgaon, Haryana."
- The Informant advised that he had sponsored a visa for Narang, and the records show that to be true: the Informant is listed as Narang's visa sponsor, and the Informant's telephone number appears as the "Sponsor Contact Phone Number."[2]

Attached as Exhibit 2 is a screen shot of the FBI database records, including Narang's photograph.[3]

7. The application information indicates that Narang is, under his visa, permitted entry into the United States until June 9, 2026. The application indicates that at the time of Narang's visa application his occupation was "computer science," his employer was "Webninjaz Technologies Pvt Ltd," and his email address was sahil.zebit@gmail.com. *See* Exhibit 2.

8. The Informant was and is cooperating with the FBI in the hope of receiving leniency in the disposition of a pending matter. The investigation in that pending matter indicates that the Informant knowingly made false statements as part of a fraud scheme, which did not involve Narang. The Informant has not yet been convicted in that pending matter and has not previously been convicted of any crimes.

October 2018

9. On October 31, 2018, the Informant told me, by telephone, that he had recently communicated with Narang and had learned the following about Narang's scheme:

- Narang operated or was associated with a call center in India, and conducted his scheme by having call center employees contact intended victims,
- the victims were generally people who had been previously victimized in other, earlier telemarketing scams,
- when contacting the victims, the callers would advise that they were able to obtain funds or refunds for the victims,
- the callers then had the victims permit access to their computers and would post information to the computer screens that led the victims to believe that their bank accounts

[2] The Informant did not sponsored Narang for a visa at the FBI's direction. The sponsorship occurred prior to the Informant becoming a source of information for the FBI.

[3] For privacy and security purposes, some information has been redacted, including the Informant's name and telephone number.

had received funds in excess of the originally promised amount,

- the callers would then direct the victims to remit the surplus funds through prepaid gift cards that would be drawn on in a manner that would result in funds being made available in India, and
- in fact, no money had been or would be sent to the victims' accounts.

10. I directed the Informant to learn additional details about Narang's scheme.

December 23, 2018 Text Exchange

11. On December 23, 2018, the Informant advised that he had recently used WhatsApp, a smartphone communication application, to communicate with Narang by text message. The Informant provided screen shots of the text message exchange. In the exchange, the Informant and Narang discuss meeting at an upcoming conference in Las Vegas.

12. In the screen shots, I saw the profile page of the person or party with whom the Informant was texting. The WhatsApp account name on the profile page was "Jai Guru Ji," and a picture purporting to be of the account user appeared on that page. The Informant identified Narang as the person in the picture, and that person is consistent in appearance with Narang's Facebook profile picture (Exhibit 1) and Narang's visa application photograph (Exhibit 2). According to that WhatsApp profile page, the number of the smartphone associated with the WhatsApp account is "650-457-9360." Finally, as described further below, when Narang entered the United States on April 20, 2019, he had in his bag a smartphone assigned that number. A screen shot of that profile page is attached as Exhibit 3.

December 26, 2018 Phone Call

13. On December 26, 2018, the Informant advised that he had recently used WhatsApp to call and speak to Narang.[4] The Informant provided an audio and video recording of the call. The Informant had placed the call with one smartphone and had recorded the call with another smartphone. During a subsequent call placed by the Informant to Narang, I was

[4] WhatsApp allows the sending of text messages and voice calls.

present. The voice I heard on the other end of the line was the same voice that I heard in the aforementioned recording.

14. In the recorded call, Narang asked whether the Informant could obtain personal identification information for individuals who had previously bought technical support, including name, phone number, address, email address, and the amount paid. Narang explained that

- his group, "we," would call the individuals, offer to refund them the money they had paid, show them images that would convince them that their accounts had received funds in excess of the intended refund amount, and direct them to return the excess,
- while no actual money would be sent to the individuals' accounts, the images they would be shown would suggest otherwise, and
- the individuals would be directed to "return" the supposed excess funds to various bank accounts in the United States, and Narang would have the money sent to him in India from those accounts.

Narang also indicated that gift cards could be used in the process of getting money from the victims.

January 3, 2019 Text Exchange

15. On January 3, 2019, the Informant advised that he had recently used Snapchat[5] to communicate with Narang by text message. The Informant provided screen shots of the text message exchange.

16. Toward the beginning of the exchange, Narang said that he would not be able to attend the conference in Las Vegas.

17. As the exchange continued, Narang inquired whether the Informant had obtained the personal identification information Narang had requested, explained that he had 20 to 30 "kids" but needed "data to scale[.]" Based on context, I interpret Narang to be saying that he had 20 to 30 people who can serve as callers for his scheme but he needs to identify prospective victims. Next, Narang said that he needed bank accounts in the United States to collect "fraud wires." Based on context, I interpret Narang to be saying that he needed

[5] Snapchat is a multimedia message application that can be used to share photographs, videos, and texts.

accounts to which he or his team can direct the money obtained from their scheme. Finally, Narang said that if the Informant could set up these sorts of accounts, he could keep 30% of the proceeds that flowed through the accounts.

January 17, 2019 Phone Call

18. On January 17, 2019, the Informant advised that he had recently used WhatsApp to call and speak to Narang. The Informant provided an audio and video recording of the call. The Informant had placed the call with one smartphone and had recorded the call with another smartphone. During a subsequent call placed by the Informant to Narang, I was present. The voice I heard on the other end of the line was the same voice that I heard in the aforementioned recording.

19. In the recorded call, Narang asked the Informant to open bank accounts and allow Narang to direct victim money, "scam money," into the account. Narang explained that the money would be coming from individuals who did not know that they had been defrauded or scammed, and that he could get $100,000 a day transferred into the Informant's accounts. Narang explained that the day after the Informant received money in an account, the money should be withdrawn and the account should be closed. Narang again offered to split the money with the Informant, this time with the Informant keeping 40% of the proceeds. Narang explained that he had previously had others, "a lot of Indian," do the same thing for him but that the manner in which their bank accounts had been set up, they could only receive small amounts.

February 4, 2019 Text Exchange

20. On February 4, 2019, the Informant advised that he had recently used WhatsApp to communicate with Narang by text message. The Informant provided screen shots of the text exchange.

21. In the exchange, the Informant advised that he would "have the accounts set up through his banker in RI." Narang responded, "Great let's get started."

February 12, 2019 Text Exchange

22. On February 12, 2019, the Informant advised that he had recently used Snapchat to communicate with Narang by text message. The Informant provided screen shots of the text exchange.

23. In the exchange, the Informant advised that he had almost completed setting up a bank account, and that all that remained was going to the bank and signing papers.

February 14, 2019 Rhode Island Phone Call

24. On February 14, 2019, at approximately 4:30, the Informant used WhatsApp to call Narang. The Informant was in Rhode Island, and the call was placed in my presence. The Informant conducted the call over his smartphone's speakerphone, and I overheard the entirety of the call. I recognized the voice on the other end of the call as the voice of the person the Informant had spoken to in the prior recorded calls.

25. In the call, the Informant said that he had a contact in Rhode Island who assisted in setting up an account in another person's name and that that contact advised that any wire transfer into the account should be kept at under $10,000 per wire. In reality, the account was a covert FBI investigative account maintained with a cooperating bank, which hereinafter is referred to as the "Fraud Account A."

26. In the call, Narang told the Informant that he should withdraw the funds in the account within two days of any wire transmission, and that efforts would be made to keep the victims from calling their banks during those two days. Narang said that once the money had been withdrawn, he would provide details about how to get him his "cut" and explained that the money would be directed to him in India through a "hawala"[6] conducted by people Narang knew in New York or Florida. Narang said that the Informant's share of the proceeds would be 30% and further explained that he would be splitting his share with others involved in the

[6] A "hawala" is generally a money transfer system whereby money is paid to an agent and that agent then instructs an associate who is located elsewhere to pay the intended recipient an equivalent sum of money and no direct transfer of funds occurs between the agent and the associate.

scheme. Narang said that the money would be coming from his "tech support" clients, but added that if the Informant was agreeable, Narang would also direct money from his "IRS" and "SSN" clients. (Based on context, I interpret Narang to be referring to other schemes he was involved in and inquiring whether the Informant would be agreeable to serving as a monetary conduit for those other schemes.)

27. In the call, Narang gave an example of how the "tech" client process worked. He explained that an individual who had previously paid $500 for computer tech support would be called and told that the $500 payment was being refunded because the tech support company was shutting down. The caller would get the individual to allow remote access to his or her computer. If the individual questioned the remote access, the caller would explain that the tech support company had previously installed software on the computer and that the software had to be removed. After remote access was established, the caller would explain that the refund had to be directed to the individual's bank account and would have the individual navigate to his or her account online. The caller would use certain software, "inspect element," to show the individual that by mistake $5,000 had been deposited into the account instead of $500, all meaning that the individual owed the caller $4,500. The caller would then have the individual deposit his or her own money into Fraud Account A via wire transfer. The caller would tell the individual not to touch his or her computer or bank account for two days after the wire had been sent. Narang explained that after two days the individual might realize that he or she had been "scammed," and that's why the money had to be withdrawn from Fraud Account A within two days.

February 15, 2019 Rhode Island Text Message

28. On February 15, 2019, I met the Informant in Rhode Island and provided him with the bank account number for Fraud Account A, the name of a fictitious person listed as the account holder (hereinafter referred to as "XX"), the routing numbers, bank address, beneficiary address, and online login id and password information for the account. In my presence, the

Informant, using WhatsApp, sent the information to Narang via text. Screen shots of those texts were taken.

Starting February 17, 2019 – Victim #1, SM

29. On February 17, 2019, the Informant advised that he had recently used WhatsApp to communicate with Narang via text. The Informant provided screen shots of the text exchange.

30. In the exchange, Narang sent an image of a wire transfer form prepared by or on behalf of SM.[7] The form listed SM's name, address, bank account number and bank name, and driver's license number. The form also listed Fraud Account A's number as the destination account number, XX as the holder of Fraud Account A, and a transfer amount of $10,000.

31. In the exchange, Narang wrote "$10k done" and inquired whether the money had arrived and whether it had been withdrawn.

32. I reviewed records associated with Fraud Account A. They showed that on February 19, 2019, Fraud Account A received $10,000 via a wire transfer from an account associated with an "SM." On February 20, 2019, from a bank in Rhode Island, I had the $10,000 withdrawn from Fraud Account A.

33. Using commercially available people locator databases and the name and address specified in the wire transfer form, I identified SM and determined her date of birth.

34. On March 7, 2019, FBI agents went to SM's home in California and spoke to her. She identified herself as SM and further identified herself through her address and date of birth, all of which matched the information I had gathered. As she spoke to the agents, she expressed reservations. She said that she had been told not to talk to anyone and would not answer any questions. She asked the agents to wait while she made a phone call. She returned to her door a short time later and told the agents that she had wired money to an account and said that the money was for a "loan." She refused to provide any further detail and would not answer any

[7] Victim are identified by first and last name initials, not their actual names.

further questions. She said she was afraid of telling them more. She took their business cards and said she would think about calling.

Starting February 27, 2019 – Victim #2, CJ

35. On February 27, 2019, the Informant advised that he had recently used WhatsApp to communicate with Narang via text. The Informant provided screen shots of the text exchange.

36. In the exchange, Narang sent an image of a wire transfer form prepared by or on behalf of CJ. The form listed CJ's name, bank account number and bank name, driver's license number, address, and phone number. The form also listed Fraud Account A's number as the destination account number, XX as the holder of Fraud Account A, and a transfer amount of $4,500.

37. In the texts, Narang asked whether the money had arrived and was told that it had. Narang subsequently wrote that his share of the first two transfers would be $10,150, and the Informant's would be $4,350.

38. I reviewed records associated with Fraud Account A. They showed that on February 25, 2019, the account received $4,500 via wire transfer from an account associated with "CJ." On February 27, 2019, from a bank in Rhode Island, I had the $4,500 withdrawn from Fraud Account A.

39. Using commercially available people locator databases and the telephone number and address specified in the wire transfer form, I identified CJ and determined her date of birth.

40. On March 7, 2019, FBI agents met CJ in Minnesota and spoke to her. CJ identified herself as CJ and further identified herself through her address, phone number, and date of birth, all of which matched the information I had gathered. CJ said that she had communicated with someone between February 12 and 25, 2019 and had been lead to wire $4,500 to an account for the purpose of correcting a computer "hack."

Starting February 28, 2019 – Victim #3, RP

41. On February 28, 2019, the Informant advised that he had recently used WhatsApp to communicate with Narang via text. The Informant provided screen shots of the text exchange.

42. In the exchange, Narang sent an image of a wire transfer form prepared by or on behalf of RP. The form listed RP's name, bank account number and bank name, address, and home phone number. The form also listed a transfer amount of $15,000.

43. In the text exchange, Narang asked whether the money had arrived, specifying that $15,000 had been wired. Narang stated that he had an additional $15,000 waiting to be sent. The Informant asked him not to send the additional sum.

44. I reviewed records associated with Fraud Account A. They showed that on February 27, 2019, the account received $15,000 via wire transfer from an account associated with "RP." On February 28, 2019, from a bank in Rhode Island, I had the $15,000 withdrawn from Fraud Account A.

45. Using commercially available people locator databases and the telephone number and address specified in the wire transfer form, I identified RP and determined his dated of birth.

46. On March 21, 2019, FBI agents spoke to RP, who resides in California, by telephone. She identified herself as "RP" and further identified herself through her address, which matched the information I had gathered. RP said that she received an email that said that her bank account had been hacked. She called the number provided in the email and spoke to a male. She subsequently communicated with that male via electronic mail, text message, and telephone. She said she was led to believe that she had caused a transfer of $30,000 into her bank account from the male's company and that she needed to return that money. To effectuate return, she said she had wired money out of her account.

March 1, 2019 – Closure of Fraud Account A

47. By February 28, 2019, three separate wires had transferred three sums of money into Fraud Account A. In a WhatsApp text communications with Narang on or about February 28, a screen shot of which the Informant provided to me, the Informant advised Narang not to send any more money to Fraud Account A and advised that the Informant's contact at the bank would be opening a new account. On March 1, 2019, Fraud Account A was closed. However, as set forth below, Narang continued to text the Informant information about anticipated targets or anticipated wire transfers.

Starting March 4, 2019 – Victim #4, WM

48. On March 4, 2019, the Informant advised that he had recently used WhatsApp to communicate with Narang via text. The Informant provided screen shots of the text exchange.

49. In the exchange, Narang sent an image of a computer screen which was open to a bank website and logged into an account. The image showed the bank's name, WM's name as the account holder, and the last four digits of the account numbers for several different accounts, including a checking account, savings account, and equity line of credit. According to that image, WM's checking and savings accounts together contained over $100,000, and the equity line of credit had an available balance of over $450,000.

50. In the text exchange, Narang told the Informant that his "office customers can pay up to 80k[.] In one go[.]" When the Informant asked if Narang had a "client" who would pay 80k for something, Narang replied "They get scammed bro[.]" In context, I interpret Narang's text message to be conveying to the Informant that $80,000 can be taken from WM or that it was anticipated that WM would be targeted for that amount. Narang also inquired when the Informant would be having a new account opened for accepting victim funds.

51. I contacted a representative of WM's bank and provide his name and the partial account numbers I saw in the image sent to the Informant. The bank representative, in turn, confirmed that WM was the holder of the partially identified accounts and further provided his date of birth and address.

52. On March 6, 2019, I went to WM's home in New York and spoke to him. He identified himself as "WM" and further identified himself through his date of birth and address, both of which matched the information I had gathered. WM told me that within the past year he had paid for computer technical support and that callers had been telling him that his Microsoft software had been compromised and would be "shutoff."

53. As we were speaking, WM received a telephone call that he recognized from caller identification as one of the aforementioned callers. WM engaged his telephone's speakerphone and answered. I overheard and recorded the call.

54. The caller, in an Indian accent, identified himself as "Roy," said he was part of a computer support team, and said he worked for a company named "Tech Support Angel." The caller said that he had previously fixed WM's computer and was calling to inquire about the computer. At my direction, WM asked "Roy" to call back in 30 minutes. "Roy" stated that he would, and the call ended.

55. Approximately 30 minutes later, WM received a call, engaged his telephone's speakerphone, and answered. I was able to overhear and recorded the call. The caller's voice matched the accent and voice of the person who had previously introduced himself as "Roy," but the caller introduced himself this time as "Jason Abbney." The caller said that he had previously called and been told to call back in 30 minutes. "Jason" said that his company was receiving information suggesting that the security software on WM's computer was not operating properly and requested that WM allow "Jason" remote access to WM's computer.

56. At my direction, WM complied and "Jason" obtained remote access. "Jason" said he was examining WM's computer and a short time later advised WM that his computer has been compromised. At some point, WM grew frustrated and, contrary to my direction, told Jason that he wished to end the call. Just before the call ended, WM asked "Jason" to again identify himself and his company and to provide a telephone number so that WM could call back. The caller now identified himself as "Jordan," identified his company as "Computer Repair," and provided a callback number.

57. I advised WM, a 95 year-old male, not to call back and discussed with him measures he could take to avoid being victimized by callers.

Starting March 7, 2019 – Victim #5, KC

58. On March 7, 2019, the Informant advised that he had recently used WhatsApp to communicate with Narang via text. The Informant provided screen shots of the text exchange.

59. In the exchange, Narang sent an image of KC's driver's license, which listed his name, address, and date of birth. Narang texted that the license belonged to a person from whom $5,000 was going to be taken. Narang sent an image of a wire transfer form that listed a partial bank account number and the full name of the bank. The form also listed Fraud Account A's number as the destination account number, XX as the holder of Fraud Account A, and a transfer amount of $5,000.

60. Using commercially available people locator databases and the information from KC's driver's license, I identified KC and determined his social security number.

61. On March 18, 2019, FBI agents went to KC's home in Arizona and spoke to him. KC identified himself as KC and further identified himself through his address, date of birth, and social security number, all of which matched the information I had gathered. KC relayed the following:

- In September 2018, he had for $500 purchased a three year computer support contract from an IT company named "Hyperion IT Solutions." The fee was billed to his credit card.
- On March 7, 2019, someone called him saying he was "Roy" from Hyperion and was calling to conduct a 90-day checkup.
- At some point, Roy "took over" KC's computer screen and then told him that the computer had problems and a fix would cost $200.
- KC suspected that he was being scammed and declined assistance. Roy told KC that if he was dissatisfied with Hyperion's service, the $500 fee would be refunded, and KC indicated that he wanted a refund.
- After KC declined Roy's offer to provide the refund via a gift card, Roy said he would process the refund through KC's bank account.
- Somehow, as Roy was processing the refund and showing KC material on KC's computer screen, KC saw a zero added to the $500 refund.

- KC specified that he believed that at some point Roy had $5000 directed from KC's account to another account.

62. During the interview, KC showed agents records associated with his account. Those records showed that on March 7, 2019, $5000 was wired from KC's account to Fraud Account A, and that on March 8, 2019, $4,955 was returned to KC's account, the original funds less certain bank fees.

March 7, 2019 – Fraud Account B

63. On March 7, 2019, to facilitate continuation of the investigation, another covert FBI investigative account was opened, and this account is hereinafter referred to as "Fraud Account B."

64. A few days prior to March 11, 2019, I provided the Informant with the bank account number for Fraud Account B,[8] the name of a fictitious person listed as the account holder (which remained "XX"), the routing numbers, bank address, beneficiary address, and online login id and password information for the account. The Informant advised that on or about March 11, he used WhatsApp to communicate with Narang via text and sent the information I had provided. Narang responded that he would no longer be directing money to Fraud Account A. Narang inquired about limits on the amount that could be sent by wire to Fraud Account B, and the Informant responded that he would check with his bank contact. The Informant provided screen shots of the text exchanges.

Starting March 11, 2019 – Victim #6, LB

65. On March 11, 2019, the Informant advised that he had recently used WhatsApp to communicate with Narang via text. The Informant provided screen shots of the text exchanges.

66. In the exchange, Narang sent an image of an outgoing wire transfer form prepared by or on behalf of an account holder. The image, a photograph, cut out part of the left margin of the form. From what could be seen, the form listed the sending bank's name and

[8] The Informant initially misstated the account number. Later, after the Informant recognized the error, he provided Narang the correct account number.

indicated that at 4:21 pm on March 8, 2019, $3,500 was wired from an account ending in "805." The form also listed Fraud Account A's number as the destination account number.

67. I called the bank that appeared on the wire transfer form to inquire about the March 8, 2019 wire transfer. The bank agent advised that she could not divulge details but would provide my telephone number to the account holder.

68. On March 12, 2019, I received a telephone call from an "LB." LB said that she had been contacted by her bank and given my telephone number. I inquired about any wire transfers that had recently been conducted from her bank account. LB relayed the following:

- Approximately two weeks ago LB began receiving calls from a person claiming to be associated with Microsoft, and on March 8, 2019 she received a voice message on her telephone stating that anti-virus software had already been downloaded on her computer and she would be billed. The message included a call back number.
- After checking her credit card records and determining that she had not been billed, LB called the number left on the message to make sure that she would not be billed in the future. The person who answered the call identified himself as "John Smith," and he had an Indian accent.
- LB told Smith that she did not want any anti-virus software and did not want to be billed. Smith had her sign into her computer, and allow him remote access for the purpose of removing the anti-virus software from the computer.
- After obtaining access, Smith said that he had uninstalled the software and then told LB to fill out a form so that he could refund the $400 she had been billed.
- At some point LB became convinced that she had entered $4000, instead of $400, on the refund form, and Smith became upset and told her that she owed him the difference. So she agreed to pay him.
- Smith told LB that she could have a $100 credit for being so cooperative, and that she therefore owed him $3500, not $3600.
- Smith asked LB to obtain a Walmart gift card to pay him, but she refused. He then provided instructions to wire money to an account that Smith said belonged to one of his friends.
- LB went to her bank and had $3,500 wired to the account Smith specified. She later learned that that money had been returned minus $10 for fees charged by her bank.

Starting March 14, 2019 – Victim #7, VL

69. On March 14, 2019, the Informant advised that he had recently used WhatsApp to communicate with Narang via text. The Informant provided screen shots of the text exchange.

70. In the exchange, Narang sent an image of an outgoing wire transfer form dated March 14, 2019 prepared by or on behalf of VL. The form listed VL's name, bank account number and bank name, and driver's license number. The form listed the Fraud Account A's number as the destination account number, XX as the holder of the Fraud Account, and a transfer amount of $24,500. (Although Fraud Account A had been closed and Narang had been given the information for the new account, Fraud Account B, it appears the schemers had not updated there information at the time of this transaction.) The form stated that the transfer was for the purchase of a vehicle.

71. In the text exchange, Narang specified that he was planning to "do a big one today."

72. Using commercially available people locator databases and VL's driver's license information, I identified VL and determined her date of birth and social security number.

73. On April 9, 2019, FBI agents went to VL's home in California and spoke to her. VL identified herself as VL and further identified herself through her address, date of birth, and social security number, all of which matched the information I had gathered. VL relayed the following:

- Roughly three to four weeks prior, she received a telephone call from a man who identified himself as "Barry Allen" and who had a thick "middle eastern" accent.
- Allen said that he wished to return funds to her and that he would need access to her computer to effectuate the return. He explained that he needed to download software onto her computer.
- Allen directed her to click on an icon on her computer, and once she did, Allen gained control over her computer.
- Allen told VL that she was owed $500 and that the money would be refunded to her in two deposits of $250.

- At a certain point, Allen directed VL to type in $250 on her computer. Allen later told VL that she had made a mistake that had resulted in more funds being sent to her than she was owed and that she would have to return the money, which amount to $24,500, to Allen's company by directing funds to a particular account, which Allen described as belonging to his company's chief executive officer.
- VL looked at her Wells Fargo account and noticed what appeared to be a $25,000 wire transfer deposit. VL subsequently had $24,500 wired to the account Allen specified.
- Later she noticed that her account had been manipulated so that $25,000 had been drawn from her savings account and transferred to her checking account. She also noticed that the wired money seemed to have returned to her account.

March 18-19, 2019 -Disposition of Money Obtained

74. On March 18, 2019, the Informant advised that he had recently used WhatsApp to communicate with Narang via text message. The Informant provided screen shots of the text exchange. In the exchange, Narang provided the Informant instructions on how to transfer cash to Narang in India. Narang directed the Informant to a person in New York City and provided the person's first name and telephone number.

75. The Informant advised that he had called the number Narang provided, had spoken to a male, and had been directed to bring the money to an address in Manhattan.

76. On March 19, 2019, I met the Informant in New York City. In my presence, the Informant used WhatsApp to call Narang. The Informant conducted the call over his smartphone's speakerphone, and I overheard the entirety of the call. I recognized the voice of the person on the other end of the line as the same voice I had heard in the aforementioned calls between the Informant and Narang. Narang told the Informant that he would receive an actual one dollar bill from the person in New York City and that he should send Narang a photograph of that bill. Narang said that the photograph would be used to obtain the money in India.

77. The Informant was outfitted with audio and video recording devices and provided $20,650, the total amount of money wired to Fraud Account A in the three wire transfers (respectively money from SM, CJ, and RP) less the Informant's 30% share. The

Informant then proceeded directly to the Manhattan address he had been provided, as I followed. I saw the Informant enter a building and depart after a short time.

78. On departing, the Informant returned directly to my company and said that he had just met the male with whom he had spoken on March 18, 2019. The Informant said that he transferred the $20,650 to the male, and he gave the Informant a one dollar bill. The audio and video recordings devices corroborated what the Informant said. In my presence, the Informant photographed the bill and using WhatsApp sent the photograph to Narang via text. The Informant then, using WhatsApp again, telephoned Narang in my presence. The Informant advised Narang that the money has been delivered to the person in New York City.

Starting April 5, 2019 – Victim #8, MS

79. On April 5, 2019, the Informant advised that he had recently used WhatsApp to communicate with Narang via text. The Informant provided screen shots of the text exchange.

80. In the exchange, Narang sent an image of an outgoing wire transfer form prepared by or on behalf of MS. The form listed MS's name, bank account number and bank name, address, social security number, and home telephone number. The form also listed XX as the holder of the Fraud Account, and a transfer amount of $5,000.

81. In the exchange, Narang asked that the money be withdrawn from the account.

82. I reviewed records associated with Fraud Account B. They showed that on April 3, 2019, the account received $5,000 via wire transfer from an account associated with "MS." On April 5, from a bank in Rhode Island, I had the $5,000 withdrawn from Fraud Account B.

83. Using commercially available people locator databases and the name, address, and social security number specified in the wire transfer form, I identified MS and determined his date of birth.

84. On April 12, 2019, FBI agents went to MS's home in Colorado and spoke to him. He identified himself as MS and further identified himself through his address, phone number, and date of birth, all of which matched the information I had gathered. MS relayed the following:

- A male with a thick Indian accent called, identified himself as "Kelvin," and said he worked for Apple.
- Kelvin said he wanted to refund MS $100 for an overpayment on his Apple care contract. MS provided Kelvin remote access to his computer.
- At Kelvin's request, MS navigated to his online bank account, and it appeared to him that $10,000 had been deposited into his account.
- Kelvin said that because of the mistaken deposit, he was going to lose his job. Kelvin asked MS to fix the mistake by wiring money back to Kelvin.
- MS wired $5000 to an account specified by Kelvin. MS said that he could only send $5,000 at a time because of limits imposed by his bank. MS sent a copy of the wire transfer form to Kelvin.
- Kelvin also asked MS to mail cash in the amount of $5,000 to a location in California, and MS did so.
- Subsequently, Kelvin called MS on other occasions and said that the money MS had sent had not been received and tried to get MS to send more money.
- MS at a certain point became suspicious, called Kelvin, and asked to speak to his supervisor. Kelvin called back a short time later, and another male was on the phone with Kelvin. That other male introduced himself as "Tim Cook" and said that he was Apple's chief financial officer. Cook assured MS that the transactions were legitimate.

Starting April 12, 2019 – Victim #9, RS

85. On April 12, 2019, the Informant advised that he had recently used WhatsApp to communicate with Narang via text. The Informant provided screen shots of the text exchange.

86. In the exchange, Narang sent an image of a wire transfer form prepared by or on behalf of RS. The form listed RS's name, bank account number and bank name, and address. The form also listed a transfer amount of $28,500.

87. In the exchange, Narang sent another image showing that a $28,500 wire transfer had been credited to Fraud Account B on April 12, 2019 and asked that it be withdrawn from the account.

88. I reviewed records associated with Fraud Account B. They showed that on April 12, 2019, the account received $28,500 via a wire transfer from an account associated with "RS." On April 18, I had the $28,500 withdrawn from Fraud Account B.

89. Using commercially available people locator databases and the address information on the wire transfer form, I identified RS and determined his date of birth.

90. On April 23, 2019, FBI agents went to RS's home in Maryland and spoke to him. He identified himself as RS and further identified himself through his address and date of birth, both of which matched the information I had gathered. RS relayed the following

- A male with an Indian accent called, identified himself as "Rajive Mathur," and said RS's social security number had been compromised and was being used for laundering money and for other crimes.
- Mathur said RS's social security number had been associated with an abandoned vehicle that was found in Texas with cocaine and blood in it.
- Mathur told RS that to protect his money, he needed to transfer all of it into federal deposit accounts for safekeeping. Mathur also told RS that he would receive a new social security number.
- Mathur provided RS with fictitious contact names and case numbers from the Social Security Administration and Department of Justice. Mathur also instructed RS not to tell anyone about the case.
- RS opened a new bank account and made numerous wire transfers to multiple accounts, using account numbers provided by Mathur. After each wire transfer was completed, RS sent an email with the confirmation receipt to an email address that Mathur supplied.

91. One of the account numbers that Mathurs provided to RS was the number for Fraud Account B. Also records supplied by RS showed that $28,500 was sent to Fraud Account B on April 12, 2019.

Starting April 15, 2019 – Victim #10, ED

92. On April 15, 2019, the Informant advised that he had recently used WhatsApp to communicate with Narang via text message. The Informant provided screen shots of the text exchange.

93. In the exchange, Narang sent an image of an outgoing wire transfer form prepared by or on behalf of ED. The form listed ED's name, bank account number and bank name, address, and driver's license number. The form also listed a transfer amount of $9,900.

94. In the text exchange, Narang inquired about whether the $9,900 had been withdrawn and sent an image showing that the $9,900 wire transfer had been credited Fraud Account B on April 12, 2019.

95. I reviewed records associated with Fraud Account B. They showed that on April 12, 2019, the account received $9,900 via wire transfer from an account associated with "ED." On April 18, 2019, I had $9,900 withdrawn from Fraud Account B.

96. Using commercially available people locator databases and the driver's license number from the wire transfer form, I identified an ED and determined his date of birth.

97. On April 22, 2019, FBI agents went to ED's home in New York and spoke to him. He identified himself as ED and further identified himself through his address and date of birth, both of which matched the information I had gathered. ED relayed the following

- A male with an Indian or Arabic accent called, identified himself as "David," and said he worked for a computer support company.
- David said ED's security license on his computer had expired and needed to be updated.
- At David's request, ED clicked on a button that appeared on his computer and entered a code that David provided. After entering the code, ED believed that David may have had control of his computer but was not certain.
- David said that too much money was deposited into ED's bank account and showed ED on his computer that ED's checking account had received a $9,900 deposit. David asked ED to return the money to David to correct the mistake and provided ED with an account number.
- ED wired $9,900 to the account specified by David.
- The following day, David called ED and told him that the $9,900 was not received. David said that only gift cards could be accepted as payment, and instructed ED to purchase $9,900 in gift cards.
- ED purchased eight gift cards valued at a total of $9,900 and provided David with the card numbers and pin codes.
- ED noticed that his checking account had a zero balance following his wire transfer and the purchase of the gift cards. Without success, ED attempted to contact David.

98. The account to which David had instructed ED to wire $9,900 was Fraud Account B.

April 20, 2019 – Narang's Arrival in the United States

99. During the weeks of April 7 and April 14, 2019, the Informant advised that he had used WhatsApp to communicate with Narang by text. The Informant provided screen shots of the text exchanges. In the texts, Narang told the Informant that he was traveling from Zurich, Switzerland to San Francisco, California and arriving on April 20, 2019. Narang also mentioned that he planned to stay in the United States for a month.

100. On April 20, 2019, I was notified by agents of the Custom and Border Protection ("CBP") that Narang had arrived that day at the San Francisco airport at approximately 6pm and had been traveling from Zurich, Switzerland.

101. CBP provided me with a photograph taken of Narang as he passed through a CPB checkpoint in the San Francisco airport. That photograph is attached as Exhibit 4, and the person photographed is consistent in appearance with the photograph in Exhibit 1 (Facebook profile page), the photographed in Exhibit 2 (visa application photograph), and the photograph in Exhibit 3 (WhatsApp profile page).

102. At the checkpoint, CBP agents interviewed Narang. He stated the following:

- he planned to stay in the United States for approximately 1 month and was planning to visit a cousin in California,
- he owns a clothing business named Bee Velvet, which has about 12 employees, and
- he owns Webninjaz, an internet affiliate marketing business, which has about 25 employees.

103. At the checkpoint, CBP agents examined Narang's baggage and found a black iPhone X with a telephone number of 650-457-9360 and a gold iPhone Max with telephone number 9999093505.

104. The telephone number for Narang's black iPhone X is identical to Narang's WhatsApp profile page, which was provided by the Informant (Exhibit 3). The telephone number for Narang's gold iPhone Max is identical to the number that Narang provided as his home phone number on his visa application (Exhibit 2).

Probable Cause

105. Based on the above, there is probable cause to believe that a group planned and on multiple occasions executed or attempted to execute a scheme to defraud, and that the scheme operated as follows:

- a telephone caller would offer to direct funds to the victim, purportedly a refund, but in fact no funds would ever be sent to the victim,
- the caller would have the victim enable remote access to the victim's computer, often explaining that the access was necessary for processing the refund or conducting a computer virus check,
- typically through the remote access to the victim's computer, the caller would lead the victim to believe that his or her bank account had received an amount far in excess of the refund amount,
- to correct the supposed over-deposit, the caller would have the victim transfer money from his or her bank account to a bank account controlled by the schemers, and
- because no refund or "excess" funds would in fact be deposited into the victim's bank account, the victim, while having been led to believe that he or she was returning excess funds, would in fact be sending the schemers his or her own funds.

106. There is also probable cause to believe that Narang was one of the conspirators. The Informant identified Narang as a party to the instances of fraud and the overall conspiracy. Recorded communications corroborate the Informant, including communications describing how the fraud was conducted and communications concerning routing of money from victims. One of Narang's smartphone call numbers, 650-457-9360, links him to the WhatsApp account through which many of the recorded communications were conducted.

Conclusion

107. Based on the above, I believe that there is probable cause to believe that Narang committed the offenses specified in paragraph 2 above.

Special Agent Craig A. Graham
Federal Bureau of Investigation

Subscribed and sworn to before
me this 29th day of April 2019,
at Providence, Rhode Island

Lincoln D. Almond
United States Magistrate Judge